Mitigating the Vulnerabilities for the Larger Infrastructures and Smaller Attention to the Cyber Security Threats in Large Scale Networks

Reshma Ashik Chauhan

Senior Research Analyst, SMRVD Security Solutions, India.

Abstract: We have seen the development and demand for seamless interconnectivity of smart devices to provide various functionality and abilities to users. Nevertheless, we also know the vulnerabilities that exist inside of it. However, these vulnerabilities normally considered for the larger infrastructures and little attention to the cyber security threats that can be resulted from the usage and power of smart devices because of IoT. The smart spaces are interconnected, with powerful smart devices (smartphones, tables, etc). We also have the backbone, the power grid that powers our nations. Those two are coming together. We present some related background and motivation seen on the development and demand for seamless interconnectivity of smart devices to provide various functionality and abilities to users.

Keywords: Data Analytics; Big Data; Classification algorithms.

1. Introduction

Although recent advancements provide many benefits to home users, it also gives rise to new security threats. We therefore need to ensure that relevant policies and tools are developed to protect the vulnerable. The concept of connected home is not only about allowing devices to be connected; it is also about "content anywhere" and information sharing [1-9]. Although this provides many advantages to the home user, but the resulting security and privacy issues not been addressed. This has been on the rather for some time in the form of Personal Networks.

In a personal context, concepts such as the Home Network and the Personal Area Network (PAN) focus on facilitating the interconnection of Personal Computers as well as other smart devices. Recent development means that other types of networks such as a Vehicular Area Network (VAN) are becoming common. The key defining characteristic of all of these networks is that the network topology relates to a geographic locality [10-24]. This connotes that the network only includes devices and systems that are present in a specific area, while at the same time the devices can be connected and reconnected seamlessly. Use of smart devices within smart environments generates an ever-increasing amount of data, often without the consent of the consumer, or without the user being fully aware of the implications

of sharing their personal data or using and sharing these devices. Hence, in some instances, a user centric-approach in designing such networks to facilitate users‘ involvement and control is needed. Researchers define the concept of a Personal Network (PN). They envisioned the personal network as a dynamic extension of the PAN to encompass the user‘s home network as well as other networks such as a VAN. A recent example of the implementation of a PN is the EU FP7 research project, webinos. This project has developed and demonstrated architecture for creating and using personal networks that span across the PAN (mobile), home and vehicle environments as well as cloud-based functionality [25-37]. The webinos project also presents a model for communicating between different personal networks.

Moreover, the smart meter on your home or business is now allowing that connectivity as well as home services or the interconnected powerful smart devices. The example of the smart grid also provides means of controlling and monitoring smart grid infrastructures via the use of portable smart device. The vulnerability of the connected home and development within the energy industry‘s new wireless smart grid will inevitably lead to lights out for everyone while the multitude of interconnected smart devices in IoT will become a hotplate for cyber-attack or robot network (botnet) and security nightmare for smart space users and possibly national infrastructures as a whole.

Latest research reported that on average one modern person own three internet-connected smart devices such as smartphone and tablet. According to market analysts, consumers spend over USD2 trillion a year on devices, services and content from three perspectives: the devices consumers use; the content, applications and services they support; and the behaviour and demographics that drive their purchasing decisions and buying patterns [38-45]. We also have seen the development and demand for seamless interconnectivity of smart devices to provide various functionality and abilities to users. While these devices provide more features and functionality, they also introduce new risks. Therefore, because of the ubiquity of smart devices, and their evolution as computing platforms, as well as the powerful processor used in smart devices has made them suitable objects for inclusion in a cyber bot. Smart devices are now widely used by billions of users due to their enhanced computing ability, practicality and efficient Internet access, thanks to the advanced of solid-state technologies. Moreover, smart devices typically contain a large amount of sensitive personal and corporate data and used in online payments and other sensitive transactions.

The wide spread use of open-source smart device platforms such as Android and third-party applications made available to the public also provides more opportunities and

attractions for malware creators. Therefore, for now and the near future smart devices will become one ofthe most lucrative targets for cybercriminals. Another more worrying impact of such hacking capability is enabling hackers use the vast resources of the home network to turn it to a botnet in order to launch a cyber-attack on national infrastructures. There are some Android based apps that when downloaded from a third party are capable of accessing the root functionality of devices and turning them into botnet components without the users' explicit consent [46-57]. People could easily and unwittingly download malware to their smart devices or fall prey to "man in the middle" attacks where data thieves pose as a legitimate body, intercept and harvest sensitive information, and then forward it to the legitimate recipient.

The main focus of this paper in twofold: firstly to provide and highlight the possible threats and vulnerability of smart devices, secondly to analyze the challenges involved in detecting mobile malware in smart devices as well as other threats within connected home ecosystem futures. The weakest link in any IT security chain is the user. The human factor is the most challenging aspect of mobile device security. Home users generally assume that everything will work just as it should, relying on a devices' default settings without referring to complex technical manuals. Therefore, service and content providers, and hardware vendors need to be aware of their responsibilities in maintaining network security and content management on the devices they provide. Service providers might also have the opportunity to provide add-on security services to complement the weaknesses of the devices.

The issue of cyber security is much closer to home environment. Hence, the problem of cyber security extends beyond computers, it also a threat to portable devices. Many electronic devices used at home are practically a computer from mobile phones, video consoles and car navigation systems. While these devices provide more features and functionality, they also introduce new risks. Attackers may be able to exploit of these technological progressions to target devices previously considered as secure.

The information stored and managed within such devices and home networks forms part of individuals Critical Information Infrastructure (CII) as identified by the POST note on cyber security in the UK. For example, an attacker may be able to contaminate your smart device with a virus, steal your mobile phone or wireless service, or access the data on your tablet. Not only do these activities have implications for your personal information, but they could also have serious consequences if you also kept corporate information on your smart device.

According to Juniper Networks report, 76 percent of mobile users are relying on their mobile devices to access their most sensitive personal information, such as online banking or personal medical information. This trend is even more noticeable with those who also use their personal mobile devices for business purposes. Nearly nine in ten (89 percent) business users, report they use their mobile device to access sensitive work-related information. Another more worrying impact is the ability of cybercriminals using the vast resources of the network to turn it to a botnet and lunch a cyber-attack on national critical infrastructures. Juniper Networks Mobile Threat Centre (MTC) reported that in 2011 there were unparalleled increase of mobile malware attacks with a 155 percent increase from the previous year across all platforms.

While it may sound overwhelming, devices such as TVs, digital picture frames, smart meters and e-readers are quite vulnerable and competent of causing problems on your network. The next few years will provide various types of malware developers to explore unlikely methods of achieving their evil goals. Smartphones are not invulnerable and Macs can get malware, such as CVE-2012-0507 vulnerability. Android-based devices suffered from more cybercriminal attacks due to their increase in usage and exposition to cyber threats. Well-established hacker groups such as the Anonymous target this exploited; it will pose a bigger threat to smart environments that protect highly sensitive data, targeting individuals for various political and financial reasons. Mobile phishing is also particularly popular among cybercriminals because wireless communications enable phishing not only via e-mail, as is the case with PCs, but also via SMS and multimedia messaging services (MMS). In the 2012 first quarterly report from Trend Micro, it has been pointed out that the large diffusion of mobile devices and the outflow of awareness on the principal cyber threats have resulted in an increase in the interest of cybercrime in the mobile sector.

2. Related Threats

Here, we provide a summary of some of the security threats associated to future connected home because of rapid increase in the availability and use of smart interconnected devices. The assumption is that the enterprise is where the big security challenges are, but home is where the hearts of consumers are. The home is becoming the battleground for developing new devices and push point for consumer electronics. The number of devices available at our disposal at home domain is increasing on daily basis. This creates a huge hole in the connectivity and security of such devices. So also is the need of these devices to interact with each other seamlessly to provide us with service that we have not dreamed of

before. In addition, it is of paramount importance to provide home users with simple interface to configure and change security requirements within the system.

Security threats and attacks to connected home infrastructures will likely come in two ways: either by or to the sensors/devices connected to the network or to the servers that gather, store, and analyze information from the sensors. Both kinds of vulnerability need consideration. From the device or sensors connected to dummy devices, they are the weakest link in the system.

Device connected to the Internet can take many forms, ranging from simple devices that measure things like temperature to video cameras that monitor the physical security of anything from homes, city streets to remote oil pipelines. Most of the data breaches in 2013 are targeting web applications, this follows with cyber espionage. These attacks are much easier on smart devices or unprotected home networks.

A recent report identified that nearly half of web applications cyber-attacks target retailers, in this case most online shopping is via personal home networks and of smart devices. One of the challenges is that simple devices or sensor devices are very inexpensive to be affordable on a mass scale, it will be vital to embed security in the device networks before they are installed, rather than trying to retrofit them later.

In past few decades, some work has been done to defend computer servers and networks from malicious attacks, but the emergence of the Internet of Things (IoT) and smart homes is forcing cyber-security experts to rethink how such assets could be protected. One of the key strategies for protection control systems was to isolate them from other networks. Now that control systems are, connected to the Internet, that approach will not work well anymore. Hence, there is a crucial need for multi-tier user-centered security system–blending safeguards for individual devices, servers, networks and applications with more powerful access controls, content management and network monitoring.

The IoT and smart home developments have created exciting new possibilities, but it can only deliver on its promises if it is reliable and trustworthy. Now is the time to start addressing these concerns. Half of mobile application transmits personal details or device information, as a results threats associated to rogue applications and social engineering expected to keep on rising.

The security risks to the enterprise associated with lost or stolen employee devices is nothing new, but the growing mobile workforce leaves these tools open to loss or theft. Out of

the 187 million compromised identities found by Symantec in 2011, about 10% (18.5 million) were as a result of a lost device

Studies show that consumers (and hence, employees) are lax about mobile phone security. A recent report from Juniper Networks states that Wi-Fi attacks are on the rise, as open connections give hackers easyaccess to social networks and email.

With emerging technologies comes new and evolved malware. Malware of itself can be of two main forms. Firstly, agents based developed and operated by government agencies, law enforcement agencies or corporate that needs to intercept and monitor a specific user, network, or service. Secondly, developed and managed by an organized criminal network or criminals who want to capitalize on the widespread distribution of malware for financial gains or other malicious intends. Smartphone security threats are increasing, according to a new Symantec report. According the Symantec report, the story of one gang earned $1 million/year using this technique. The criminals donot need a huge number of phones to do it.

Unclear corporate policies to address new technologies while supporting employee benefits that come with the increasing consumerization of IT may not seem like a security threat. Many enterprises are overwhelmingly supportive of employee choices when it comes to the variety of devices and applications available to them to boost productivity. Yet the same companies have been slow to adopt corporate policies that address the specific threats that these emerging technologies bring into the workplace. Employees were seen as the most likely source of an attack, this follows by consumers accounting for 57% and 10% respectively.

The connected home ecosystem both provides and consumes internal services as well as consuming external services. By definition, these services provide some value to the user or the other elements of the network. An attacker could obtain the benefit provided by these services. An example of theft of an external service would be smartphone malware that uses the device‘s mobile broadband connection, for which the user may be billed. Since computation considered as internal service, an example of theft of this service would be an attacker using a target device to perform computational operations such as mining crypto-currency.

A relatively recent possible objective of the attacker is unauthorized control of cyber-physical systems. In the context of the connected home futures ecosystems, the term cyber-physical refers to any computational system, which forms part of the network but also has the

capability to control external physical infrastructure. This will mostly likely also have the Remote accessibility characteristic.

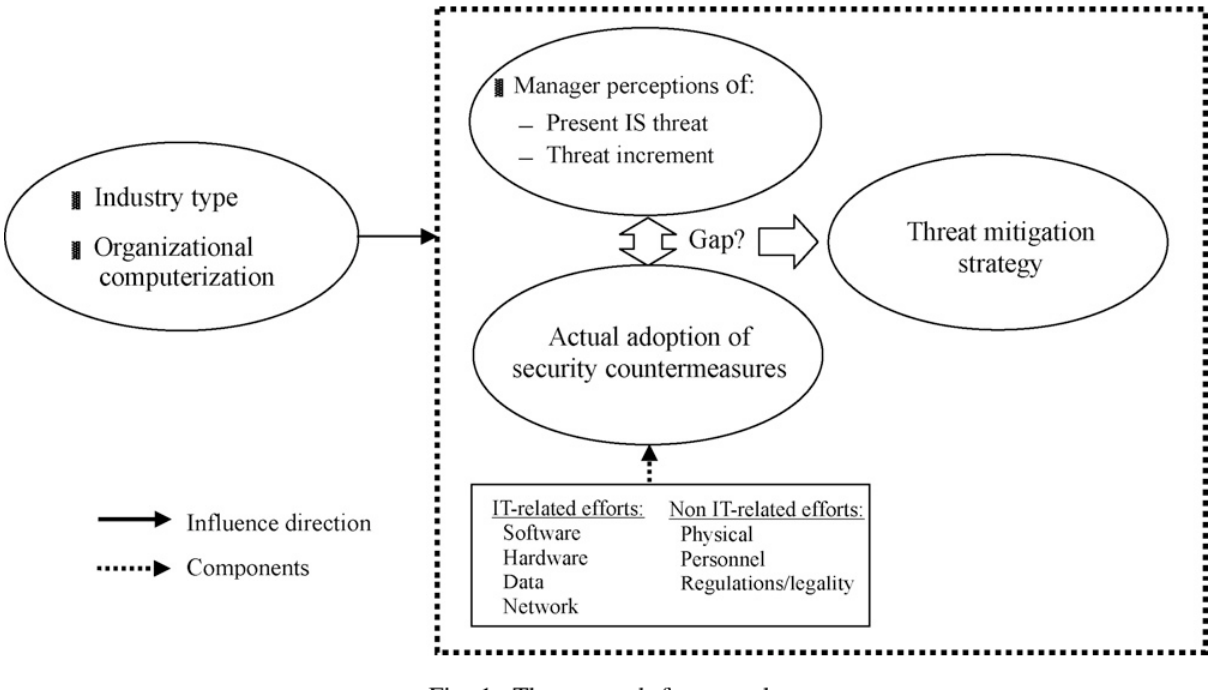

Figure 1. Prevailing Threats and counter measures in Cybersecurity

For example, cyber-physical systems include various types of (future) smart meters, smart home appliances such as smart refrigerators, lighting controllers or heating, ventilation and air-conditioning (HVAC) systems, which can control aspects of the physical environment. Cyber-physical systems focus on enabling a user to control his or her physical environment and usually provide this functionality through the personal network. Therefore, unauthorized control of cyber-physical infrastructure would be a possible objective for an attack on the personal network. However, as the number of smart cyber-physical systems increases, this attack objective is likely to become a relevant concern in the connected home ecosystem futures. Therefore, the brief summary of some of threats presented above provides a useful starting point for efforts to enhance the security of current and future personal networks.

3. Conclusions

Today‘s users utilize their mobile smart devices for everything from accessing emails to sensitive transactions such as online banking and payments. As users become more dependent on their mobile devices as digital wallets, this creates a very lucrative target for cybercriminals, and a huge challenge for security experts. Mobile smart device users can expect to see a significant malware increase on finance related applications, such as mobile

banking. The paper discussed the issue of connected home ecosystem futures in reference to various threats that makes such systems vulnerable and a lucrative target for cybercriminals. In the near future, cyber security experts will see an increasing threat to the home infrastructures as the key target and challenge for them to address as cybercriminals will find such systems easy to use and infiltrate. This is also true to mobile smart device users who can expect to see a striking increase in malware and notable advancements in malware-related attacks, particularly on the Android platform as the user base grow exponentially.

References

[1] A Oulasvirta, A. Pihlajamaa, J. Perki, D. Ray, T. Vhkangas, T. Hasu, N. Vainio, and P. Myllymki. Long-term effects of ubiquitous surveillance in the home. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, pages 40–50. ACM, 2012.

[2] Amir Rahmati, Earlence Fernandes, Kevin Eykholt, and Atul Prakash. Tyche: Risk-based permissions for smart home platforms. arXiv preprint arXiv:1801.04609, 2018.

[3] P.N. Dawadi, D.J. Cook, M. Schmitter-Edgecombe, and C. Parsey. Automated assessment of cognitive health using smart home technologies. Technology and health care, 21(4): 323–343, 2013.

[4] Vinod Varma Vegesna (2022). "Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues," International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[5] Vinod Varma Vegesna (2022). "Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions," Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[6] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[7] Hamid Ali Abed Al-Asadi and et al., "Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network", Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[8] Hamid Ali Abed Al-Asadi and et al., "A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[9] Vinod Varma Vegesna (2022). “Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks,” International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[10] Ejaz Ahmed, Ibrar Yaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications, 23(5):10–16, 2016.

[11] T.Y. Chung, I. Mashal, O. Alsaryrah, T.H. Hsu, C.H. Chang, and W.H. Kuo. Design and implementation of light-weight smart home gateway for social web of thing. In Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on, pages 425–430. IEEE, 2014.

[12] Vinod Varma Vegesna (2022). “Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling businesses to create more dynamic applications,” International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[13] Vinod Varma Vegesna (2022). “Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems,” Irish Interdisciplinary Journal of Science and Research, Vol. 6, Iss. 4, Pages 70-86, October-December 2022, doi: 10.46759/iijsr.2022.6409.

[14] Vinod Varma Vegesna (2021). “Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage,” Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[15] Hamid Ali Abed Al-Asadi, et al., “Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement”, Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[16] Hamid Ali Abed Al-Asadi and et al., “ Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[17] Hamid Ali Abed Al-Asadi, (2022) “1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[18] Vinod Varma Vegesna (2021). “A Highly Efficient and Secure Procedure for Protecting

Privacy in Cloud Data Storage Environments," International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[19] Vinod Varma Vegesna (2021). "The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing," International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[20] Sid Stamm, Zulfikar Ramzan, and Markus Jakobsson. Driveby pharming. In International Conference on Information and Communications Security, pages 495–506. Springer, Berlin, Heidelberg, 2006.

[21] A. Antonini, F. Maggi, and S. Zanero. A practical attack against a knx-based building automation system. In Proceedings of the 2nd International Symposium on ICS and SCADA Cyber Security Research 2014, pages 53–60. BCS, 2014.

[22] Todd Kennedy and Ray Hunt. A review of wpan security: attacks and prevention. In Proceedings of the international conference on mobile technology, applications, and systems, page 56. ACM, 2008.

[23] Vinod Varma Vegesna (2021). "The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes," International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[24] Vinod Varma Vegesna (2020). "Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications," Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[25] Vinod Varma Vegesna (2019). "Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes", Indo-Iranian Journal of Scientific Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[26] Vinod Varma Vegesna (2018). "Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy", Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[27] Vinod Varma Vegesna (2017). "Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis," International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[28] Philipp Jovanovic and Samuel Neves. Practical cryptanalysis of the open smart grid protocol. In International Workshop on Fast Software Encryption, pages 297–316. Springer, Berlin, Heidelberg, 2015.

[29] A. Brauchli and D. Li. A solution based analysis of attack vectors on smart home systems. In Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on, pages 1–6. IEEE, 2015.

[30] HAPCAN. HAPCAN: about project - basic information, 2017.

[31] Subhojeet Mukherjee, Hossein Shirazi, Indrakshi Ray, Jeremy Daily, and Rose Gamble. Practical dos attacks on embedded networks in commercial vehicles. In Information Systems Security, pages 23–42. Springer, 2016.

[32] Vinod Varma Vegesna (2023). "Adopting a Conceptual Architecture to Mitigate an IoT Zero-Day Threat that Might Result in a Zero-Day Attack with Regard to Operational Costs and Communication Overheads," International Journal of Current Engineering and Scientific Research, Volume-10, Issue-1, Pages 9-17.

[33] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[34] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[35] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[36] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[37] Vinod Varma Vegesna (2023). "Methodology for Mitigating the Security Issues and Challenges in the Internet of Things (IoT) Framework for Enhanced Security," Asian Journal of Basic Science & Research, Vol. 5, No. 1, January-March 2023, Pages 85–102, doi: 10.38177/ajbsr.2023.5110.

[38] Vinod Varma Vegesna (2023). "Secure and Reliable Designs for Intrusion Detection Methods Developed Utilizing Artificial Intelligence Approaches," International Journal of Current Engineering and Scientific Research, Volume-10, Issue-3, Pages 1-7.

[39] Vinod Varma Vegesna (2023). "A Critical Investigation and Analysis of Strategic Techniques Before Approving Cloud Computing Service Frameworks," International Journal of Management, Technology and Engineering, Volume XIII, Issue IV, April 2023, Pages 132-144.

[40] Anatolij Bezemskij, George Loukas, Richard J Anthony, Diane Gan, et al. Behaviour-based anomaly detection of cyberphysical attacks on a robotic vehicle. 2016.

[41] J. Vanderauwera A. Puppe. Research project: Homeplug security, 2010.

[42] B. Tasker. Vulnerability: Infiltrating a network via powerline (HomePlugAV) adapters, 2014.

[43] S. Dudek. HomePlugAV PLC: practical attacks and backdooring, 2015.

[44] Echelon Corporation. 90 million energy-aware lonworks devices worldwide, 2010.

[45] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner. Smart locks: Lessons for securing commodity internet of things devices. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pages 461–472. ACM, 2016.

[46] Aur´elien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In In proceedings of the 18th Annual Network and Distributed System Security Symposium. The Internet Society, 2011.

[47] Hongwei Du. Nfc technology: Today and tomorrow. International Journal of Future Computer and Communication, 2(4): 351, 2013.

[48] Mathy Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS). ACM, 2017.

[49] Vinod Varma Vegesna (2016). "Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain," International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[50] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[51] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach", European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[52] Vinod Varma Vegesna (2015). "Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security," International Journal of

Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[53] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, "Fuzzy Logic approach to Recognition of Isolated Arabic Characters", International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[54] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, "Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers," Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[55] L. Coppolino, V. DAlessandro, S. DAntonio, L. Levy, and L. Omano. My smart home is under attack. In Computational Science and Engineering (CSE), 2015 IEEE 18th International Conference on, pages 141–151. IEEE, 2015.

[56] Joshua Wright. Killerbee: practical zigbee exploitation framework. In 11th ToorCon conference, San Diego, 2009.

[57] R. Jenkins, R. Shapiro, S. Bratus, T. Goodspeed, R. Speers, and D. Dowd. Short paper: speaking the local dialect: exploiting differences between ieee 802.15. 4 receivers with commodity radios for fingerprinting, targeted attacks, and wids evasion. In Proceedings of the 2014 ACM conference on Security and privacy in wireless and mobile networks, pages 63–68. ACM, 2014.